

Claims

- [c1] 1. A method for securing software to reduce unauthorized use of the software, the method comprising: providing software including data representing digital content; associating at least one identifier with the software prior to distribution of the software, the identifier being detectable by an authorized representative to request authentication of the software; and distributing the software with the at least one identifier to a user.
- [c2] 2. The method of claim 1 wherein the software is self activating and self authenticating in conjunction with an authorized representative located on or in the user device.
- [c3] 3. The method of claim 1 wherein the digital content is selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a maga-

zine, and data representing a book.

- [c4] 4. The method of claim 1 wherein the identifier is hidden from the user.
- [c5] 5. The method of claim 1 wherein the identifier is tamper resistant to the user.
- [c6] 6. The method of claim 1 wherein the at least one identifier is embedded within a file of at least one component of the software.
- [c7] 7. The method of claim 1 wherein the at least one identifier is a binary code.
- [c8] 8. The method of claim 1 wherein the at least one identifier is encrypted.
- [c9] 9. The method of claim 1 wherein the step of distributing the software comprises electronically distributing the software.
- [c10] 10. The method of claim 1 wherein the step of distributing the software comprises distributing the software on a computer readable storage medium.
- [c11] 11. The method of claim 1 further comprising:
performing a process to determine whether an attempted access to the software is authorized based on

detection of the at least one identifier.

[c12] 12. The method of claim 11 wherein the step of performing a process comprises:
determining whether the attempted access to the software is authorized based on registration information associated with the software.

[c13] 13. The method of claim 11 wherein the step of performing a process comprises:
determining whether the attempted access to the software is authorized based on registration information associated with the software and registration information associated with a user device.

[c14] 14. The method of claim 1 further comprising:
communicating registration information to an authorized representative of the software;
generating at least one authentication code based on the registration information; and
associating the authentication code with the software.

[c15] 15. The method of claim 14 wherein authorized representative functions are implemented by a user device.

[c16] 16. The method of claim 14 wherein authorized representative functions are implemented by software.

- [c17] 17. The method of claim 14 wherein authorized representative functions are implemented by hardware.
- [c18] 18. The method of claim 14 wherein authorized representative functions are implemented by hardware and software.
- [c19] 19. The method of claim 1 wherein the at least one identifier is included in a filename for at least one component of the software.
- [c20] 20. The method of claim 19 wherein the identifier is selected from the group consisting of the filename, a filename prefix, a filename suffix, a filename extension, a filename extension prefix, and a filename extension suffix.
- [c21] 21. The method of claim 19 wherein the identifier is tamper resistant to the user.
- [c22] 22. The method of claim 19 wherein the identifier is hidden to the user.
- [c23] 23. A method for securing software to reduce unauthorized use of the software, the method comprising:
providing software including data representing digital content;
associating a plurality of identifiers with the software

prior to distribution of the software, at least one identifier being detectable by an authorized representative to request authentication of the software; and distributing the software with the plurality of identifiers to a user.

[c24] 24. The method of claim 23 wherein the software is self activating and self authenticating in conjunction with an authorized representative located on or in the user device.

[c25] 25. The method of claim 23 wherein at least one of the identifiers is an activation code that must be entered by the user prior to transferring the software.

[c26] 26. The method of claim 23 wherein the digital content is selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.

[c27] 27. The method of claim 23 wherein at least one of the at least one identifiers is hidden from the user.

[c28] 28. The method of claim 23 wherein at least one of the

at least one identifiers is tamper resistant to the user.

- [c29] 29. The method of claim 23 wherein the at least one identifier is embedded within a file of at least one component of the software.
- [c30] 30. The method of claim 23 wherein the at least one identifier is a binary code.
- [c31] 31. The method of claim 23 wherein the at least one identifier is encrypted.
- [c32] 32. The method of claim 23 wherein the step of distributing the software comprises electronically distributing the software.
- [c33] 33. The method of claim 23 wherein the step of distributing the software comprises distributing the software on a computer readable storage medium.
- [c34] 34. The method of claim 23 further comprising:
performing a process to determine whether an attempted access to the software is authorized based on detection of the at least one identifier.
- [c35] 35. The method of claim 34 wherein the step of performing a process comprises:
determining whether the attempted access to the software is authorized based on registration information as-

sociated with the software.

- [c36] 36. The method of claim 34 wherein the step of performing a process comprises:
determining whether the attempted access to the software is authorized based on registration information associated with the software and registration information associated with a user device.
- [c37] 37. The method of claim 23 further comprising:
communicating registration information to an authorized representative of the software;
generating at least one authentication code based on the registration information; and
associating the authentication code with the software.
- [c38] 38. The method of claim 37 wherein authorized representative functions are implemented by a user device.
- [c39] 39. The method of claim 37 wherein authorized representative functions are implemented by software.
- [c40] 40. The method of claim 37 wherein authorized representative functions are implemented by hardware.
- [c41] 41. The method of claim 37 wherein authorized representative functions are implemented by hardware and software.

[c42] 42. The method of claim 23 wherein the at least one identifier is included in a file name for at least one component of the software.

[c43] 43. The method of claim 42 wherein the identifier is selected from the group consisting of a filename, a filename prefix, a filename suffix, a filename extension, a filename extension prefix, and a filename extension suffix.

[c44] 44. The method of claim 42 wherein the identifier is tamper resistant to the user.

[c45] 45. The method of claim 42 wherein the identifier is hidden to the user.

[c46] 46. A method for securing software to reduce unauthorized use having at least one authorized representative entity installed on or in a user device, the method comprising:
associating at least one identifier with the software to designate the software for protection from unauthorized use;
detecting the at least one identifier using the authorized representative installed on or in the user device;
determining whether the user device is authorized to access the software using the authorized representative

entity installed on or in the user device; and
controlling access to the software based on whether the
user device is determined to be authorized.

[c47] 47. The method of claim 46 wherein the software is self
activating and self authenticating in conjunction with an
authorized representative located on or in the user de-
vice.

[c48] 48. The method of claim 46 further comprising:
determining whether the user device is authorized to ac-
cess the software using a remotely located authorized
representative entity in combination with the at least one
authorized representative entity installed on or in the
user device.

[c49] 49. The method of claim 46 wherein the at least one au-
thorized representative entity installed on or in the user
device comprises a computer chip.

[c50] 50. The method of claim 46 wherein the at least one au-
thorized representative entity installed on or in the user
device comprises program instructions executed by a
microprocessor.

[c51] 51. The method of claim 50 wherein the program in-
structions comprise an operating system component.

- [c52] 52. The method of claim 50 wherein the program instructions comprise an application program.
- [c53] 53. The method of claim 50 wherein the program instructions comprise a driver for a secondary device.
- [c54] 54. The method of claim 46 wherein the step of determining whether the user device is authorized comprises: comparing registration information associated with the user device to registration information associated with the software.
- [c55] 55. The method of claim 54 wherein the registration information associated with the software is embedded within an authentication code.
- [c56] 56. The method of claim 54 wherein the registration information associated with the software is encrypted.
- [c57] 57. The method of claim 54 wherein the registration information includes hardware information.
- [c58] 58. The method of claim 57 wherein the registration information includes hardware information associated with a unique user device.
- [c59] 59. The method of claim 57 wherein the hardware information includes a serial number.

- [c60] 60. The method of claim 57 wherein the registration information includes hardware information associated with a group of user devices.
- [c61] 61. The method of claim 46 wherein the authorized representative entity is installed by a manufacturer of the user device.
- [c62] 62. The method of claim 46 wherein the authorized representative entity is installed from a computer readable storage medium.
- [c63] 63. The method of claim 46 wherein the authorized representative entity is installed from the software.
- [c64] 64. The method of claim 46 wherein the authorized representative entity is downloaded to the user device.
- [c65] 65. The method of claim 46 wherein the authorized representative entity is transferred to the user device from a network.
- [c66] 66. The method of claim 46 wherein the step of controlling access comprises preventing the software from being transferred to a second user device.
- [c67] 67. The method of claim 46 wherein the step of controlling access comprises preventing the software from being transferred to a user device if at least one authorized

representative is inaccessible.

[c68] 68. The method of claim 46 wherein the step of controlling access comprises preventing the software from being installed on a user device if at least one authorized representative is not present.

[c69] 69. The method of claim 46 wherein the step of controlling access comprises preventing the software from being executed by the user device.

[c70] 70. The method of claim 46 wherein the step of controlling access comprises providing limited access to the software.

[c71] 71. The method of claim 46 wherein the software comprises digital content.

[c72] 72. The method of claim 71 wherein the software is selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.

[c73] 73. The method of claim 46 wherein the software com-

prises instructions for generating at least one authentication code based on registration information associated with the user device.

[c74] 74. The method of claim 73 wherein the software comprises instructions for encrypting the authentication code.

[c75] 75. A method for securing software to reduce unauthorized use of the software, the method comprising:
providing software including data representing digital content;
detecting an identifier associated with the software indicating that protection from unauthorized use is desired;
communicating with an authorized representative entity to determine whether a user device attempting to access the software is authorized to access the software; and
controlling access to the software based on whether the user device is authorized.

[c76] 76. The method of claim 75 wherein the software is self activating and self authenticating in conjunction with an authorized representative located on or in the user device.

[c77] 77. The method of claim 75 wherein the identifier associated with the software is contained within a filename

for the software.

[c78] 78. The method of claim 75 wherein the authorized representative entity is a hardware device.

[c79] 79. The method of claim 75 wherein the step of communicating with the authorized representative entity comprises communicating with at least one software module associated with the user device.

[c80] 80. The method of claim 75 wherein the authorized representative entity is installed on the user device.

[c81] 81. The method of claim 75 further comprising:
generating an authentication code based on registration information associated with the user device; and
associating the authentication code with the software.

[c82] 82. The method of claim 75 wherein the step of communicating comprises:
generating an authentication code based on registration information associated with the user device; and
comparing the authentication code with a previously generated authentication code associated with the software to determine if the user device is authorized.

[c83] 83. The method of claim 82 wherein the step of comparing the authentication code comprises determining if at

least a portion of system information associated with the user device matches system information encoded within the authentication code associated with the software.

[c84] 84. The method of claim 81 wherein the registration information includes hardware-specific information.

[c85] 85. The method of claim 75 wherein the authorized representative entity is installed on or in the user device.

[c86] 86. The method of claim 75 wherein the digital content is selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.